A Privacy-enabled Solution for Sharing Social Data in Ad-hoc Mobile Networks

Slawomir Grzonkowski, and Peter M. Corcoran, Member, IEEE

Abstract—There is an enormous growth of the use of mobile devices and the social Web. Thus the users want to exchange their social data easily by using their phones and PDAs. We show that existing solutions put the users at security and privacy risks. Then, we describe our protocol for exchanging users’ social data. We demonstrate that enables better security and privacy for exchanging social data. In addition we show that our solution causes lower data overhead for the participants.

I. INTRODUCTION

Over the last decade we have experienced an enormous growth of the use of mobile phones. These devices have become an important part of our lives and everyday’s activities. The today’s mobile phones offer the possibility of managing social data such as social networks, photos, professional and personal calendars. Thus, a requirement that two users want to share or exchange this information has become important. However, mobile phones are produced by many vendors. Thus, they offer different hardware parameters that support a number of incompatible data transmission standards. This causes interoperability problems that were addressed by applications such as bu.mp™ [9]. The bu.mp project enables users to share their social data using mobile phones produced by different vendors. In this paper, we show that this solution solves the interoperability problem. However, it introduces a number of privacy and security issues that we describe. We also demonstrate how they can be effectively solved using existing web standards and a secure authentication service that we previously developed [8].

II. REVIEW OF EXISTING SOLUTION

To enable interoperability, in solutions such as bu.mp™ [9], there is a requirement of a Third Trusted Party (TTP). Its aim is to match two users and to route data between them. A typical protocol works in the following way:

1. Two users requests the social data exchange
2. Each mobile phone sends its location, exact time and page that is currently displayed to TTP
3. TTP uses its match algorithm to pair two mobile phones
4. TTP routes all the information between the phones

The work presented in this paper was supported (in part) by the Lion project supported by Science Foundation Ireland under Grant No. RSF0840 and Enterprise Ireland under Grant No. REI 1005. A method and apparatus for authenticating a user is a pending patent.

This approach causes a number of security and privacy problems. Firstly, it offers a centralized architecture, which is more prone to Denial of Service (DOS) attacks than distributed architectures. Centralized solutions also have single points of failures. Secondly, a TTP is able to collect all the routed information. Some providers also explicitly inform users that they do it to improve user’s experience. However, the user has no control over the stored information, which contains contacts, private pictures and data from the user’s social network portals. Finally, there is a possibility that two users who did not intend to communicate will be connected: there is a random element in the match algorithm. The possibility of this situation is small, but it can happen at crowded places such as conferences. In this case, random users would be able to access the content that they are not supposed to preview.

III. IMPROVED PROTOCOL AND ITS ELEMENTS

A. Social web

In our solution we take advantage of the Friend-of-a-Friend (FOAF) vocabulary [1]. FOAF was created to support publication of machine-readable user profile descriptions, including online social networks. The complete vocabulary specifies about 60 elements that belong to several categories: FOAF Basics, Personal Info, OnlineAccounts / IM, Project and Groups, Documents and Images.

FOAF can be adopted to access control through the use of the foaf:knows property, which specifies that a given individual knows another one. Although the FOAF vocabulary does not support trust levels, such extensions were proposed in various extensions, for example in the FOAFRealm project [2].

Due to the lack of authentication information in the initial vocabulary, FOAF needed extensions to provide authentication services. For this reason, with a foaf:openid property containing information about users' OpenID logins, was added to the vocabulary. Although this property can be used for providing authentication, its usability is marginal: OpenID has been perceived as a convenient, but insecure authentication method. FOAFRealm [2], which provided a FOAF-based authentication service, uses the foaf:mbox property as user logins. In addition, to increase privacy, this system stores only foaf:mbox_sha1sum. Therefore, the value of foaf:mbox is never revealed to strangers.

The vocabulary also does not support any property for storing passwords. Thus, to provide authentication, FOAFRealm introduced xfoaf:password_sha1sum to it. During the authentication process, passwords provided by the users are compared with their corresponding cryptographic password hashes stored in the user's profile at the server side.

This way of authentication does not provide strong security. Someone who possesses the user's hash may perform a...
dictionary attack, and also this method is prone to phishing [3]. To address those issues we implement our FOAF-based authentication using a Zero-Knowledge Proof protocol [4].

B. Zero Knowledge Proof Authentication Protocol

The zero-knowledge proof (ZKP) term has been formalized by Goldwasser, Micali, and Rackoff [4]. It describes a group of challenge-response authentication protocols, in which parties are required to prove the correctness of their secrets, without revealing these secrets. Such protocols exist for any NP-set, provided that one-way functions exist [4]. The use of zero-knowledge proofs as a mean of proving identity was first proposed by Fiege et al. [5]. There are many modifications of ZKP protocols. For example Guillou and Quisquater [6] proposed how to lower the bandwidth and memory requirements; Schnorr [7] described an alternative that uses the discrete logarithm problem. Our implementation uses a protocol based on isomorphic graphs [8].

C. Protocol Overview

We note that Step 5 of the presented protocol is based on our previous work in the context of ZKP authentication for mobile devices [8].

Due to the lack of space we will present more detailed results and our implementation in the full version of this paper.

D. Security and other limitations

The main limitation of our architecture is that both devices must have external IP addresses for the exchange. This requirement is, however, satisfied if they use 3G technologies. Also, there is still a need for TTP, but it does not provide data routing. Thus, in our architecture, TTP causes a lower data overhead than existing solutions [9]. We also note that our protocol does not require users to expose their privacy to the third parties, even TTP. The users, in their FOAF profiles publish parts of data that they want to become public. Only these profiles are displayed to the authenticating parties. Because of using FOAF, the users can see each other’s names and pictures. Thus they have the possibility of approving or rejecting the other party before they decide to exchange more social data. Only if both of them approve the other party, their public keys and IPs are exchanged by the matching service.

IV. CONCLUSIONS

In this paper we presented a novel method of sharing social data for mobile phones. Our method provides interoperability in a similar way to other state-of-the-art solutions [9]. However, it offers better security and privacy of exchanged data. Although in the proposed protocol we used a Third Trusted Party, we still achieved better scalability than existing solutions.

REFERENCES